



Black Hat
Black Hat Briefings
Black Hat Training
Black Hat Windows Security

THE DAWNING OF AN INDUSTRY

Since the Black Hat Briefings was first introduced in 1997, it has quickly become the premiere event and indispensable resource for the computer security industry.

This media kit serves as your guide for using the Black Hat Briefings to reach a highly targeted and influential market.

On the following pages, you will find information about the Black Hat Briefings:

MISSION: How and why the Black Hat Briefings serves the computer security arena

LEADERS: The knowledgeable and experienced people who have made the Black Hat Briefings possible

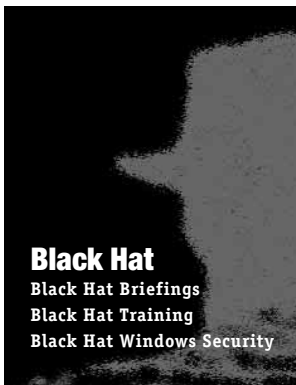
COVERAGE: Topics that have been covered in past Black Hat Briefings Conferences

SUPPORTERS: The industry leaders who support the Black Hat Briefings

CALENDAR: Schedule of Black Hat events

CONTACTS: The people who can help you make the most of your participation at the Black Hat Briefings





THE MISSION

Black Hat Briefings was originally founded in 1997 by Jeff Moss to fill the need of computer security professionals to better understand the security risks to their computers and information infrastructures by potential threats. To do this, the Black Hat Briefings assembles a group of vendor neutral security professionals and let them speak candidly about the problems businesses face, and the solutions they see to those problems. No gimmicks, no sales pitches, just straight talk by people who make it their business to explore the ever changing security space.

At every conference, the Black Hat Briefings delivers to its core audience of IT, network security experts, consultants and administrators new developments on the vital security issues facing organizations with large networks and mixed operating systems. Current hot topics include Distributed Denial of Service attacks (DDos), computer forensics, honey pots, format string vulnerabilities, incident response, secure programming techniques, security tool selection and more. Attendees gain intelligence in a face to face with the people developing the tools used by and against hackers.

The Black Hat Briefings' intense sessions bring to light the security and mis-configuration problems confronting organizations and network administrators where security gets put off in lieu of constant network growth and upgrades. Our speakers discuss the strategies involved in correcting existing problems and speak towards what you can expect in the future.

With unmatched depth and focus at the heart of the computer security community, the Black Hat Briefings is positioned to be the indispensable knowledge base for smart, informed decision making and practices in the age of information technology.





THE LEADERS: PAST AND PRESENT SPEAKERS

Chris Abad	Jason Garms	David Litchfield	Martin Roesch
David Ahmad	Ed Gerck	Jim Litchko	Rooster
Rich Alu	J.D. Glaser	Loki	Route
Chip Andrews	Chris Goggans	Thomas Lopatic	Todd Sabin
Ivan Arcé	Ian Goldberg	Terry Losonsky	Daiji Sanai
Ofir Arkin	David Goldman	Teresa Lunt	Mike Schiffman
Wouter Aukema	Sarah Gordon	Todd MacDermid	Eugene Schultz
John Bailey	Jennifer Granick	Andrew Malyshev	Eric Schultze
James Bamford	Ron Gula	Bruce K. Marshall	Winn Schwartzau
Batz	Job De Haas	Hal McConnell	Edward G. Schwartz
Jay Beale	Robert Hansen	John McDonald	Cory Scott
Marshal Beddoe	HalVar Flake	Paul McNabb	Saumil Shah
Mike Beekey	Hobbit	Kevin McPeake	Walter Gary Sharp
Michael Bednarczyk	Greg Hoglund	Gregory S Miles	Peter Shipley
Macy Bergoon	Dr. Jeffrey A. Hunker	Paul Mobley	Adam Shostack
Eric Birkholz	Brent Huston	Arthur Money	Simple Nomad
Blake	Stuart Hyde	Ron Moritz	Sir Distic
Scott Blake	Tom Jackiewicz	Dr. Mudge	Chad Skipper
Kate Borten	George Jelatis	Clinton Muggle	Ed Skoudis
David Bovee	Jeff Jonas	Timothy Mullen	Sluggo
Eric Brandwine	Jericho	Munge	Brian Snow
Dominique Brezinski	Joey	Jeff Nathan	Dug Song
Max Caeceres	Mark Kadrich	Wilfred A. Nathan	Space Rogue
Caesar	Dan Kaminsky	José Nazario	Lance Spitzner
Yu-Min Chang	Ray Kaplan	Tim Newsham	Peter Stephenson
Richard Clarke	Rob Karas	Pierre Noel	John Tan
Chey Cobb	Diana Kelly	Brian Oblivion	G. Alec Tatum, III
Miles Connley	Karen Khanna	Thomas Olofsson	Anne-Marie Tenholder
Scott Culp	Martin Khoo	William Ozier	Richard Thieme
William R. Cheswick	Max Kilger	Palante	Jeff Thompson
Steven M Christey	Kingpin	David Papas	Dean Turner
Jon David	Larry Korba	Padgett Peterson	Daniel VanBelleghem
John Davis	Dan Kurc	Ian Poynter	Andrew van der Stock
BK DeLong	George Kurtz	Priest	Huang-Yu Wang
Kevin Depeugh	Lee Kushner	Tom Ptacek	Ira Winkler
Theo DeRaadt	John Kutzschebauch	QMaster	Fyodor Yarochkin
Renaud Deraison	Last Stage of Delerium	Rain Forest Puppy	
Dave Dittrich	Research Group	Marcus Ranum	
William Dixon	Paul Leach	Jeremy Rauch	
Todd Feinman	David LeBlanc	Gordon Reichard Jr.	
Emmanuel Gadaix	Chieh-Chun Lin	Patrick Richard	

Presentations by these speakers are available at: www.blackhat.com.



COVERAGE: TOPICS THAT HAVE BEEN COVERED

Alternatives to Honeypots or the dtk
An Analysis of the Wired Equivalent Privacy Protocol
ARP Vulnerabilities: Indefensible Local Network Attacks?
Attacking and Defending BIND / DJBDNS DNS Servers
Automated Penetration Testing
Cracking WEP Keys
CVE Behind the Scenes: The Complexity of Being Simple
DOG of WAR: Attack Box Design
Fnord: A Loadable Kernel Module for Defense and Honeypots
The Future of Internet Worms
Grabbing User Credentials via W2k ODBC Libraries
GSM / WAP / SMS Security
Hardening .htaccess Scripts in Apache Environments.
Introducing X: Playing Tricks with ICMP
Layer 2 Attacks
Polymorphism and Intrusion Detection Systems
Promiscuous Node Detection Using ARP Packets
The RAZOR Warez
Researching Secrets, Part I & II
rfp.labs: New Toys in the Works
The Siphon Project: An Implementation of Stealth Target Acquisition and Information Gathering Methodologies
Snort
SQL Security Revisited
Systems Management in an Untrusted Network: Dealing with Backups, Monitoring, Administration, and Logging in the DMZ
Top 25 Overlooked Security Configurations on Your Switches and Routers
Reducing the Costs of Vulnerability Assessment Using Nessus 1.2
Building a Blind IP Spoofed Port Scanning Tool
Key Legal Implications of Computer Network Defense
Solving Network Mysteries
Wireless LAN Security
Mirror::Image The Attrition Web Defacement Mirror
The Honey Net Project
Hit Them Where It Hurts: Finding Holes in COTS Software
Gateway Cryptography: Hacking Impossible Tunnels through Improbable Networks with OpenSSH and the GNU Privacy Guard.
UNIX Assembly Codes Development for Vulnerabilities Illustration Purposes
Falling Dominos
Countering the Insider Threat with the Autonomic Distributed Firewall (ADF)
Paradigms Lost: Engineering vs. Risk Management
The Three Truths of Computer Security
Post Mortem of a Rootkit Attack
Web Hacking
Overall Security Review of GSM Infrastructure
IDS Benchmarking
IPSec in a Windows 2000 World
Stealth Network Techniques: Offensive and Defensive.
Remote Web Application Disassembly with ODBC Error Messages
Web Assessment Tools
Breaking In Through The Front Door
Non-common Architectures buffer Overflows
Restrict Anonymous and the Null User
Why Government Systems Fail at Security
Incident Response in a Microsoft World
Null Sessions, MSRPC, and Windows 2000
Healthcare and New Federal Security Protections
Safeguarding your Business Assets through Understanding of the Win32API
Virtual Private Problems: A Broken Dream
Defense in Depth: Winning in Spite of Yourself (aka "Foiling JD")
Plenty of Coppers in Change
Auditing The Security of Applications.
Defending Your Network with Kerberos.
Getting Rooted and Never Knowing It: What happens When You Can't Protect Your Kernel
What is Involved in a Forensic Effort, and What You Can Do To Improve Your Environment to Yield the Maximum Results
Strategies for Defeating Distributed Attacks
Issues Surrounding International Computer Crime Laws.



ICMP Usage In Scanning
 Advanced Buffer Overflow Techniques
 Casing the Joint: What We Already Know About Your Network
 Malicious Information Gathering
 Routers, Switches & More: The Glue That Binds Them All Together
 Intrusion Detection and Network Forensics.
 Auditing NT
 International Legal Issues Surrounding Computer Hacking
 Responding to Cyber Threats
 Internet Age: Why Security Architectures Fail (The Story of the Maginot Line Under Attack)
 Computer Crime: The Law Enforcement Perspective with Case Studies
 Advanced Windows NT Security
 Modern NetWare Hacking
 Appliance Firewalls: A Detailed Review
 Over the Router, Through the Firewall, to Grandma's House We Go
 Auditing NT—Catching Greg Hoglund
 Security Issues Affecting Internet Transit Points and Backbone Providers
 Security Issues With Implementing and Deploying the LDAP Directory System
 Building a Forensic Toolkit That Will Protect You From Evil Influences
 Overview of Certification Systems: x.509, CA, PGP and SKIP
 VPN Architectures: Looking at the Complete Picture
 Introduction to Cyber Forensic Analysis
 Secure sDNS solutions
 Firewall
 Burglar Alarms and Booby Traps
 Mistakes and blunders: A Hacker Looks at Cryptography
 1000 Hackers in a Box: Failings of "Security Scanners"
 Viruses in the Information Age
 Hope, Hype, Horrors... E-Commerce Explored
 How Responsive Are Vendors To Security Problems When They Aren't Being Pressured By Someone Threatening To Go Public?
 Towards A Taxonomy of Network Security Testing Techniques.
 Security Ideas from All Over
 Internet Mapping Project
 Total BS Security: Business-based Systems Security.
 Protecting America's Cyberspace: Version 1.0 of the National Plan
 Open Source Monitoring
 Putting Intrusion Detection into Intrusion Detection Systems
 Forensic Issues in Hacker Prosecutions
 Taxonomy of Intrusion Detection Systems
 Building a Security Response Process
 Overlooked Local Attack Techniques
 Managing the External Environment
 Competative Intelligence
 The Issues Surrounding the Hiring of "hackers"
 How to REALLY Secure the Internet.
 Mistakes and Blunders: A Hacker Looks at Cryptography.
 Secure Coding, Problems with Maintain Source Trees and Secure Design Philosophies
 Information Security: Beyond the Hype
 Penetrating NT Networks Through Information Leaks and Policy Weaknesses
 Convergence—Every Man (and Woman) a Spy
 Cell Phone Security: a History and the Sate of the Art
 Who are the Enemies of Computer and Network Security?
 SOCKS, PPTP & IPSec: Implementation & Futures
 An Overview of a TCP/IP Internals and Its Security Strengths and Weaknesses
 Real World VPN Implementation Security Issues.
 What's Different about Evidence in Computer Crime Litigation
 Security As An Enabler for New Business Opportunities—The Business Value of Security
 Security with the NTLM++ Protocol
 Open Network PKI Design Issues or "Business as Usual"
 Statistical Analysis of Reusable Passwords and Recommendations
 Trusted Operating System Technology in Web-based Computing
 Introducing the Time Based Security Model and Applying Military Strategies to Network and Infrastructural Securituies
 How to REALLY Secure the Internet
 Defeating Network Intrusion Detection
 Firewalls: Not enough of a good thing
 Internet Attack Methodologies
 Meet The Enemy
 Secure Coding Practices and Source Code Analysis
 Secure Implementations of ActiveX in a Corporate Environment
 Security Implications of Distributed Network Management
 TCP/IP Insecurities
 Why Cryptograpy is Harder Than it Looks
 Securing Your Network with Free Utilities
 Code Reviews: Making them Worthwhile
 Denial of Service Attacks, and Defensive Strategies
 Who Are The Real Black Hats?
 Building the Business Case for Management for Increased Security

Black Hat
Black Hat Briefings
Black Hat Training
Black Hat Windows Security

SUPPORTERS: PAST AND PRESENT SPONSORS

Argus Systems Group
Asita Technologies
Aventail
Bindview
Cambridge Technology Partners
Checkpoint
Computer Associates
Counterpane Systems
Cryptek
Intrusion.com

Microsoft
National Computer Security Center
Network Flight Recorder
Price Waterhouse Coopers
Secure Computing
Security Focus
SingCert
Stonesoft
Telenisus
TruSecure Corporation



Black Hat
Black Hat Briefings
Black Hat Training
Black Hat Windows Security

MEDIA SPONSORS: PAST AND PRESENT

Asia Computer Week	Private & Wireless Broadband
Broadband Solutions	SC Magazine
Business Security Advisor	Security Administrator
Communications News	Smart Partner
Computerworld Hong Kong	Sys Admin
Federal Computer Week	Telecommunications
Information Security Bulletin	Telephony
Information Security Magazine	Virus Bulletin
Interactive Week	Windows 2000 Magazine Network

ACW

**BUSINESS
SECURITY**
ADVISOR MAGAZINE

BROADBAND
SOLUTIONS

Communications News

**INFORMATION
SECURITY**
BULLETIN

COMPUTERWORLD
HONG KONG

**INFORMATION
SECURITY**

Private & Wireless
Broadband
Technologies serving commercial buildings and the multiworking industry

Interactive **Week**
THE INTERNET'S NEWSPAPER

SC
SECURITY
MAGAZINE

Sm@rtPartner
THE ONLY WAY TO BUILD SOLUTIONS

Security
ADMINISTRATOR

**Sys
Admin**
the journal for UNIX
systems administrators

TELEPHONY

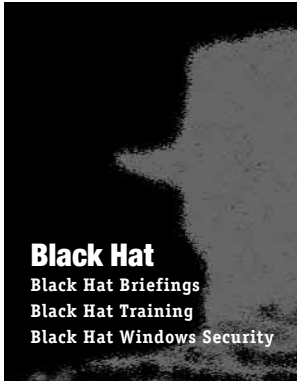
TELECOMMUNICATIONS

Windows2000
MAGAZINE
NETWORK

Federal Computer Week

VIRUS
BULLETIN





CALENDAR

Black Hat currently holds 5 conferences a year on 3 different continents. Speakers and attendees travel from all over the world to meet and share in the latest advances in computer security.

Black Hat Briefings World Tour:

Nov 2001	Amsterdam	Black Hat Briefings and Training <i>Training: 1 day, 4 different topics</i> <i>Briefings: 2 days, 2 tracks</i>
Feb 2002	New Orleans	Black Hat Briefings and Training: Windows Security <i>Training: 2 days, 4 different topics</i> <i>Briefings: 2 days, 3 tracks</i>
Fall 2002	Asia	Black Hat Briefings and Training
Nov 2002	Europe	Black Hat Briefings and Training

We look forward to seeing you there! Visit us at www.blackhat.com for updates and online presentations

How we have grown*:

1997	110
1998	320
1999	680
2000	1400
2001	1600

*figures are from the Black Hat Briefings US shows—
they do not include attendance from the international conferences





Black Hat
Black Hat Briefings
Black Hat Training
Black Hat Windows Security

CONTACT INFORMATION

Black Hat, Inc.
2606 Second Avenue, No 406
Seattle, WA 98105
t: 206.790.3628
f: 866.899.6225
<http://www.blackhat.com>

General Questions:	info@blackhat.com
Paper Submissions:	cfp@blackhat.com
Speaker Liason:	speaking@blackhat.com
Advertising and Sponsorship:	carl@blackhat.com
Press Relations:	press@blackhat.com
Registration related questions:	registration@blackhat.com
Graphics & Publications:	ping@blackhat.com

Past Black Hat Briefings presentations (video, audio and the original materials) are available for review, non-gratis at: www.blackhat.com





Black Hat
Black Hat Briefings
Black Hat Training
Black Hat Windows Security

JEFF MOSS
PRESIDENT & CEO, BLACK HAT, INC.

Jeff Moss is the founder and organizer of the Black Hat Briefings, a computer security conference and training company that deals with the technical issues of secure implementations of networks and applications. Staffed by “hackers”* of the highest skill level, this conference was created to provide hard information and a realistic assessment of technology as seen by those in the trenches. The Black Hat Briefings are held worldwide on three continents: North America, Europe and Asia. Past speakers have included the Assistant Secretary of Defense, Art Money, as well as some of the leading names in the most technical aspects of computer security worldwide.

Through this forum Mr. Moss has established global relationships in law enforcement and professional security companies, as well as with the computer underground's best hackers. This unique exposure and respect from both communities allows Mr. Moss to speak honestly and objectively on the security problems companies face when implementing technology.

In a past life Mr. Moss was a director at Secure Computing Corporation, and helped form and grow their Professional Services Department. In his capacity of developing and delivering consulting products, Mr. Moss has worked in Taipei, Tokyo, Singapore, Sydney, and Hong Kong. Prior to SCC, Mr. Moss worked for Ernst & Young, LLP as a manager in their Information System Security division.

Mr. Moss has presented at: OSS '95 Open Source Solutions, The Forbes CIO Technology Symposium, Access All Areas '96 in London, North America CACS '98, Comdex '98, The National Information System Security Convention in '98 and '00, Software Development Expo '98, PC Expo '99, CSI Net Sec '99, and Fortune Magazine's CTO Conference in '00. In addition he speaks regularly at smaller industry security seminars. Mr. Moss helps to organize “Meet the Enemy” sessions as seen at computer security gatherings worldwide including the annual Computer Security Institute conference.

Mr. Moss speaks to the media regularly about computer security, privacy and technology and has appeared in such media as CNN Fn, NPR Radio, Forbes Magazine, Fortune, Business Week, PC World, the New York Times, Wired Magazine, National Law Journal, Internet Underground Magazine, New Media Magazine, and Phrack Magazine.

Mr. Moss graduated with a BA in Criminal Justice, and halfway through law school, he went back to his first love, computers, and started his first IT consulting business in 1995. He is CISSP certified, and a member of the American Society of Law Enforcement Trainers.

* “Hackers” – a non-criminal computer security expert.

